REMARKS

The Examiner has rejected Claims 1, 3, 9-13, 15, 21-25, 27, and 33-36 under 35 U.S.C. 102(e) as being anticipated by Hoene (U.S. Publication No. 2002/0199116). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims.

With respect to the independent claims, the Examiner has relied on the following excerpts from the Hoene reference to make a prior art showing of applicant's claimed "change logging logic operable to log changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history" (see this or similar, but not necessarily identical language in the independent claims).

> "[0025] Virus protector 100 with scan function 102 uses virus definitions 104 to detect viruses at all levels of server communication with first client 20 and/or other devices, as well as network clients 24. Quarantine monitor 120 comprises a registry for tracking virus-infected client computers and which virus they each were infected with, and when the infection occurred. Quarantine monitor 120 also tracks virus-susceptible client computers, such as those without an up-to-date virus scan and/or those with disabled virus protection such as disabled virus protector 34. This information may be tracked cumulatively and used for detecting patterns in virus infection, detection and eradication. In combination with network operating system 62, quarantine monitor 120 identifies virus-susceptible client computers and virus-infected client computers for preventing their communication with server 22 and network clients 24, including which clients tend to infect the network system and/or fail to maintain virus protection. Finally, server virus monitor 64 includes blocking mechanism 128, which acts in cooperation with network operating system 62 for preventing or terminating a client-server connection for a specified client computer that is virus-susceptible or virus-infected. Operation of blocking mechanism 128 is reflected in and managed by quarantine monitor 120." (Hoene, Paragraph 0025 - emphasis added)

> "[0036] A system and method for network virus exclusion of the present invention isolates virus-susceptible clients and infected clients from a server of a network and from other network clients to prevent virus transmission throughout the network. Placing those clients in quarantine prevents virus transmission from those quarantined client computers. Moreover, requiring all other client computers to maintain full time virus protection prevents

> rampant virus transmission from an infected client computer. **Finally, by tracking the addresses of client computers that fail to maintain virus protection and/or which regularly incur virus infections,** a network administrator can take further measures against the perpetrators, such as closely scrutinizing activities of those client computers as well as denying the client computer's network computing privileges for a period of time." (Hoene, Paragraph 0036 - emphasis added)

Applicant respectfully asserts that the excerpts from Hoene relied upon by the Examiner teaches the use of "... a registry for tracking virus-infected client computers and which virus they each were infected with, and when the infection occurred" (emphasis added). The excerpts from Hoene continue to teach "track[ing] virus-susceptible client computers, such as those without an up-to-date virus scan and/or those with disabled virus protection" (emphasis added). However, the excerpts from Hoene simply fail to disclose "change logging logic operable to log changes to said update status field to create a change history in an update status tracking database" (emphasis added), as claimed by applicant. In addition, Hoene's disclosure of "tracking the addresses of client computers that fail to maintain virus protection and/or which regularly incur virus infections" (emphasis added) simply fails to meet a technique "to enable identification of weaknesses within update status management based on the change history" (emphasis added), as claimed by applicant.

Further, the Examiner has relied on the following excerpts from the Hoene reference to make a prior art showing of applicant's claimed technique "wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner" (see this or similar, but not necessarily identical language in the independent claims).

> "[0030] **First client 20 reports the results of its virus scan to server 22 (step 162). Server 22 determines whether a virus was detected (step 170).** If no virus was detected, then server 22 permits authorized access for first client 20 to server 22 and the network (step 172). However, if a virus was detected in step 170, then server 22 logs client address 32 for identification of first client 20 and terminates the limited connection of first client 20 to server 22 (step 174). Following step 174, first client 20 cleans and removes the virus with a virus cleaner and

repeats the virus scan (step 176). After virus disinfection step 176, step 162 is repeated in which first client 20 reports the results of its virus scan to server 20. When a successful virus scan report is sent to server 20 (i.e., no virus detected, as in step 170), then server 22 permits authorized access to network for first client 20 (172)." (Hoene, Paragraph 0030 - emphasis added)

"[0035] If the date of the virus definitions in the virus scan report from first client 20 fails to meet the date criteria set by server 22, then in step 258 server 22 requires first client 20 to update its virus definitions and repeat the virus scan. Step 258 optionally includes step 259 in which server 22 automatically downloads the updated virus definition file to first client 20 and requests first client 20 to complete an additional virus scan. Following the updating step 258, server 22 queries whether first client 20 has complied with the virus update request (step 260). If the client has not complied with the server update request, then in step 262 the limited connection between the server 22 and first client 20 is terminated. On the other hand, if first client 20 complied with the server request to update the virus definitions and successfully repeated the virus scan, then first client 20 participates in step 256 in which server 22 completes the connection between first client 20 and server 22 for authorized access to the network. Finally, in step 270, before the next log on to server 22 by first client 20, server 22 reminds first client 20 to update its virus definitions, schedules a virus definition update, and/or initiates a virus definition update for first client 20." (Hoene, Paragraph 0035 - emphasis added)

Applicant respectfully asserts that the excerpts from Hoene relied upon by the Examiner fail to fully disclose applicant's claimed invention. For instance, Hoene discloses a technique where the "[s]erver 22 determines whether a virus was detected (step 170)" (emphasis added) from "the results of its virus scan" (emphasis added). Additionally, Hoene teaches that "[w]hen a successful virus scan report is sent to server 20 (i.e., no virus detected, as in step 170), then server 22 permits authorized access to network for first client 20 (172)" (emphasis added). However, having the server check the virus scan results for viruses, as disclosed by the Hoene excerpts, fails to even suggest a technique "wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner" (emphasis added), as claimed by applicant.

Also, Hoene discloses that "[i]f the date of the virus definitions in the virus scan report from first client 20 fails to meet the date criteria set by server 22, then in step 258 server 22 requires first client 20 to update its virus definitions and repeat the virus scan"

(emphasis added). Again, the excerpts from Hoene simply fail to even suggest a technique where "said update status field associated with said computer file is changed to correspond to said current malware scanner" (emphasis added), as claimed by applicant.

Furthermore, the Examiner has relied on the following excerpts from the Hoene reference to make a prior art showing of applicant's claimed technique "wherein said update status alert includes one or more of: (i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and (ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status" (see this or similar, but not necessarily identical language in the independent claims).

> "[0030] First client 20 reports the results of its virus scan to server 22 (step 162). Server 22 determines whether a virus was detected (step 170). If no virus was detected, then server 22 permits authorized access for first client 20 to server 22 and the network (step 172). However, if a virus was detected in step 170, then server 22 logs client address 32 for identification of first client 20 and terminates the limited connection of first client 20 to server 22 (step 174). Following step 174, first client 20 cleans and removes the virus with a virus cleaner and repeats the virus scan (step 176). After virus disinfection step 176, step 162 is repeated in which first client 20 reports the results of its virus scan to server 20. When a successful virus scan report is sent to server 20 (i.e., no virus detected, as in step 170), then server 22 permits authorized access to network for first client 20 (172)." (Hoene, Paragraph 0030 - emphasis added)
>
> "[0035] If the date of the virus definitions in the virus scan report from first client 20 fails to meet the date criteria set by server 22, then in step 258 server 22 requires first client 20 to update its virus definitions and repeat the virus scan. Step 258 optionally includes step 259 in which server 22 automatically downloads the updated virus definition file to first client 20 and requests first client 20 to complete an additional virus scan. Following the updating step 258, server 22 queries whether first client 20 has complied with the virus update request (step 260). If the client has not complied with the server update request, then in step 262 the limited connection between the server 22 and first client 20 is terminated. On the other hand, if first client 20 complied with the server request to update the virus definitions and successfully repeated the virus scan, then first client 20 participates in step 256 in which server 22 completes the connection between first client 20 and server 22

> for authorized access to the network. Finally, in step 270, before the next log on to server 22 by first client 20, server 22 **reminds first client 20 to update its virus definitions, schedules a virus definition update, and/or initiates a virus definition update for first client 20.**
>
> 0036] A system and method for network virus exclusion of the present invention isolates virus-susceptible clients and infected clients from a server of a network and from other network clients to prevent virus transmission throughout the network. Placing those clients in quarantine prevents virus transmission from those quarantined client computers. Moreover, requiring all other client computers to maintain full time virus protection prevents rampant virus transmission from an infected client computer. Finally, by tracking the addresses of client computers that fail to maintain virus protection and/or which regularly incur virus infections, **a network administrator can take further measures against the perpetrators, such as closely scrutinizing activities of those client computers as well as denying the client computer's network computing privileges for a period of time."** (Hoene, Paragraphs 0035-0036 - emphasis added)

Applicant respectfully asserts that the excerpts from Hoene relied upon by the Examiner simply fail to even suggest any use of an "update status alert", as claimed by applicant. Hoene discloses a "[f]irst client 20 report[ing] the results of its virus scan to server" (emphasis added) and the "server 22 log[ing] client address 32 for identification of first client" (emphasis added). In addition, Hoene teaches that the "server 22 reminds first client 20 to update its virus definitions, schedules a virus definition update, and/or initiates a virus definition update for first client" (emphasis added). In addition to these actions performed by the client and server, the excerpts from Hoene above disclose that "a network administrator can take further measures against the perpetrators, such as closely scrutinizing activities of those client computers as well as denying the client computer's network computing privileges for a period of time" (emphasis added).

The excerpts from Hoene, however, simply fail to even suggest a technique "wherein said update status alert includes one or more of: (i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and (ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status" (emphasis added), as claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the above reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 3 et al., the Examiner has relied on the following excerpts from the above reference to make a prior art showing of applicant's claimed technique "wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners."

> "[0033] After first client 20 notifies server 22 of a virus infection in step 206, server 22 may take an optional secondary pathway. In the secondary pathway, server 22 marks first client 20 as suspect (step 220), and then intensively monitors activity of first client 20 by more aggressively scanning files written by suspect first client 20 (step 222).
>
> [0034] Finally, another exemplary embodiment of a method 250 of network virus exclusion of the present invention is shown in FIG. 5. Method 250 includes a first step 252 in which first client 20 initiates its log onto server 22 with a user name and/or password, and a valid virus scan report. If first client 20 is an authorized user and certifies a valid virus scan to server 22, then server 22 grants first client 20 a limited connection to server 22. However, before releasing first client 20 to authorized access to the network, server 22 determines if the date of virus definitions in the virus scan report were updated as of a specified date (step 254). In step 256, if the date of the virus definitions in the virus scan report meets the date criteria set by server 22, then server 22 establishes an authorized client--server connection with first client 20.

> [0035] If the date of the virus definitions in the virus scan report from first client 20 fails to meet the date criteria set by server 22, then in step 258 server 22 requires first client 20 to update its virus definitions and repeat the virus scan. Step 258 optionally includes step 259 in which server 22 automatically downloads the updated virus definition file to first client 20 and requests first client 20 to complete an additional virus scan. Following the updating step 258, server 22 queries whether first client 20 has complied with the virus update request (step 260). If the client has not complied with the server update request, then in step 262 the limited connection between the server 22 and first client 20 is terminated. On the other hand, if first client 20 complied with the server request to update the virus definitions and successfully repeated the virus scan, then first client 20 participates in step 256 in which server 22 completes the connection between first client 20 and server 22 for authorized access to the network. Finally, in step 270, before the next log on to server 22 by first client 20, server 22 reminds first client 20 to update its virus definitions, schedules a virus definition update, and/or initiates a virus definition update for first client 20." (Hoene, Paragraphs 0033-0035 - emphasis added)

Applicant respectfully asserts that the excerpts from Hoene relied upon by the Examiner merely teach that the "first client 20 initiates its log onto server 22 with a user name and/or password, and a valid virus scan report" (emphasis added). In addition, Hoene discloses that "server 22 marks first client 20 as suspect (step 220), and then intensively monitors activity of first client 20 by more aggressively scanning files written by suspect first client 20" (emphasis added). However, supplying a valid virus scan report to the server and having the server aggressively scan files simply fails to meet a technique "wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners" (emphasis added), as claimed by applicant.

Again, the foregoing anticipation criterion has simply not been met by the above reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

In addition, with respect to Claim 2 et al., the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over Hoene, in view of Waldin (U.S. Patent No. 6,094,731). Specifically, the Examiner has relied on the following excerpts from Waldin to make a prior art showing of applicant's claimed technique "wherein said update status field is included as a property field within said computer file."

> '7. In step 45, authentication module 12 packages the encoded contents of file 4, i.e., "attaches" the encoded contents to the original file 1 using a transmission specific format. For example, in the case of Internet e-mail, which consists of header fields followed by the e-mail body, the encoded contents of file 4 are attached to the e-mail as a header field. An example of this is given infra.' (Waldin, Col. 5, lines 21-27 - emphasis added)

Applicant respectfully asserts that the excerpts from Waldin relied upon by the Examiner teaches that "the encoded contents of file 4 are attached to the e-mail as a header field" (emphasis added). However, Waldin fails to disclose a technique "wherein said update status field is included as a property field within said computer file" (emphasis added), as claimed by applicant.

Moreover, with respect to Claims 5, 17, and 29, the Examiner relied upon the following excerpts from Waldin to make a prior art showing of applicant's claimed technique "wherein said combined file is a file compressed combination of said update status file and said computer file."

> '7. In step 45, authentication module 12 packages the encoded contents of file 4, i.e., "attaches" the encoded contents to the original file 1 using a transmission specific format. For example, in the case of Internet e-mail, which consists of header fields followed by the e-mail body, the encoded contents of file 4 are attached to the e-mail as a header field. An example of this is given infra.' (Waldin, Col. 5, lines 21-27 - emphasis added)
>
> "The e-mail with a digitally signed set of hash values looks like:
> From: me@here.net
> To: you@there.net
> Subject: something interesting
> X-NAVHashes: RlbHRhQ2F0YWxvZz4NCg==
> X-NAVHashSignature: dHA6Ly8xNTUuNjQdHATa==

When in the course of human events ..." (Waldin, Col. 6, lines 1-9 - emphasis added)

Applicant respectfully asserts that the excerpts from Waldin relied upon by the Examiner merely teach that the 'authentication module 12 packages the encoded contents of file 4, i.e., "attaches" the encoded contents to the original file 1 using a transmission specific format' (emphasis added). However, attaching encoded "X-NAVHashes ... [and] X-NAVHashSignature..." (emphasis added) to "the e-mail as a header field" simply fails to even suggest a technique "wherein said combined file is a file compressed combination of said update status file and said computer file" (emphasis added), as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claim 37 below, which is added for full consideration:

"wherein said update status alert triggers an automatic update to said malware scanner in accordance with one of administrator preferences and user preferences" (see Claim 37).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P495).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100